



Complaint Referral Form Internet Crime Complaint Center

Victim Information

Name: Carl Volz

Are you reporting on behalf of a business? Yes

Business Name: SingularDTV GmbH

Is the incident currently impacting business operations? No

Age: 50 - 59

Address: Poststrasse 30

Address (continued): 6300 Zug

Suite/Apt./Mail Stop:

City: Zug

County:

Country: Switzerland

State: [None]

Zip Code/Route: 6300 Zug

Phone Number: 7086010261

Email Address: cvolz@breaker.io

Business IT POC, if applicable:

Other Business POC, if applicable:

Financial Transaction(s)

Transaction Type: Other

If other, please specify: cryptocurrency transfer

Transaction Amount: \$2000000

Transaction Date: 05/06/2021

Was the money sent? Yes

Victim Bank Name: n/a

Victim Bank Address:

Victim Bank Address (continued):

Victim Bank Suite/Mail Stop:

Victim Bank City:

Victim Bank Country: United States of America

Victim Bank State New York

Victim Bank Zip Code/Route: n/a

Victim Name on Account:

Victim Account Number:

Recipient Bank Name: n/a

Recipient Bank Address:
 Recipient Bank Address (continued):
 Recipient Bank Suite/Mail Stop:
 Recipient Bank City:
 Recipient Bank Country: [None]
 Recipient Bank State [None]
 Recipient Bank Zip Code/Route:
 Recipient Name on Account:
 Recipient Bank Routing Number:
 Recipient Account Number:
 Recipient Bank SWIFT Code:

Description of Incident

Provide a description of the incident and how you were victimized. Provide information not captured elsewhere in this complaint form.

Criminal somehow acquired access to email of company's general counsel, interceded in email chain between general counsel and former employee with whom a settlement agreement was being negotiated, created a false email account with a name highly similar to the former employee's email and created a rule in the general counsel's email account directing all future emails in the chain to go to the false email account. General counsel unknowingly corresponded with this false account for several months, with the false email account exhibiting knowledge of non-public details of relationships and events that bolstered general counsel's belief that he was communicating with the former employee. False email account even refused to sign settlement documents for more than 2 months, citing personal family commitments. Suddenly last week fake email account resurfaced on same email chain and asked to sign the agreement and receive settlement funds as quickly as possible. Due to intrapersonal and company political dynamics, general counsel was prohibited from phoning the former employee to confirm his change of heart and was instructed to proceed with getting settlement agreement signed. Fake email account signed and returned documents with signatures that closely matched the former employee's signature and approximately \$2MM worth of a cryptocurrency tokens called SNGLS and SNGJ tokens were transmitted to the wallet addresses provided by the false email account. When Swiss managing director of company reached out to the former employee the next day to get him to sign additional documents required to recognize the settlement, the email went to the correct address as the managing director had no such "rule" created in his account and only had the original, correct email account in his email system. The former employee responded that he had neither signed the agreement nor received any payment and the company realized that it had been the victim of a scam. Company's IT vendor tracked the email to an address in England: 260 Bath Road, Slough, Berkshire, England, which is the headquarters of a company called O2, the second largest mobile network in the UK.

Which of the following were used in this incident? (Check all that apply.)

- ☒ Spoofed Email
- ☐ Similar Domain
- ☒ Email Intrusion
- ☐ Other Please specify:

Law enforcement or regulatory agencies may desire copies of pertinent documents or other evidence regarding your complaint.

Originals should be retained for use by law enforcement agencies.

Other Information

If an email was used in this incident, please provide a copy of the entire email including full email headers.

Email of original employee is arielevcohen@gmail.com. Fake email account which deceived us was arielevvycohen@gmail.com. Note the addition of an additional "y" in the fake account. Former employee's middle name begins with a "Y".

Are there any other witnesses or victims to this incident?

No.

If you have reported this incident to other law enforcement or government agencies, please provide the name, phone number, email, date reported, report number, etc.

None -- talked to NYPD but they told us to contact FBI.

☐ Check here if this an update to a previously filed complaint:

Who Filed the Complaint

Were you the victim in the incident described above? No

If not, please provide us with your contact information:

Name: Carl Volz

Business Name: SingularDTV GmbH

Phone Number: 7086010261

Email Address: cvolz@breaker.io

Digital Signature

By digitally signing this document, I affirm that the information I provided is true and accurate to the best of my knowledge. I understand that providing false information could make me subject to fine, imprisonment, or both. (Title 18, U.S. Code, Section 1001)

Digital Signature: Carl Volz

Thank you for submitting your complaint to the IC3. Please save or print a copy for your records. ***This is the only time you will have to make a copy of your complaint.***